Thiago M. Coelho, SBN 324715
thiago@wilshirelawfirm.com
Shahin Rezvani, SBN 199614
shahin.rezvani@wilshirelawfirm.com
Jennifer M. Leinbach, SBN 281404
jennifer.leinbach@wilshirelawfirm.com
Reuben Aguirre, SBN 319699
reuben.aguirre@wilshirelawfirm.com
Chumahan B. Bowen, SBN 268136
chumahan.bowen@wilshirelawfirm.com
WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd., 12th Floor
Los Angeles, California 90010
Telephone: (213) 381-9988
Facsimile: (213) 381-9989

Attorneys for Plaintiff and Proposed Class

UNITED STATES DISTRICT COURT

FOR THE CENTRAL DISTRICT OF CALIFORNIA

YVETTE PRICE, individually, and on behalf of all others similarly situated,

Plaintiffs,

vs.

FIRST FINANCIAL SECURITY, INC., a Delaware corporation; and DOES 1 through 100, inclusive,

Defendants.

Case No.

CLASS ACTION

COMPLAINT

DEMAND FOR JURY TRIAL

Plaintiff Yvette Price, ("Plaintiff"), individually, and on behalf of the class defined below, bring this class action complaint against Defendant First Financial Security, Inc. ("First Financial") and Doe Defendants are referred to as ("Defendants") and allege as follows:

INTRODUCTION

1. This class action seeks to redress Defendants' unlawful, negligent, and reckless disclosure of more than 105, 764 clients' Personally Identifiable Information (PII) and Protected Health Information (PHI), in violation of Insurance Information and Privacy Protection Act ("IIPPA"), Ins. Code, § 791.01, *et seq.*, California's Unfair Competition Law, Cal. Bus. & Prof. Code §§ 17200, *et seq.* (the "UCL"), the California Consumer Privacy Act, Cal. Civ. Code § 1798.150, *et seq.* ("CCPA"), common law claims for negligence, breach of contract, breach of implied contract, breach of the implied covenant of good-faith and fair dealing, and invasion of privacy.

2. Defendant, a national insurance agency, offers financial security products to individuals and families, including a suite of insurance products, financial planning tools, and educational services, all marketed as a means to build, protect, and preserve wealth. Specifically, Defendants markets life insurance policies, including term life, whole life, and universal life insurance, as well as Indexed Universal Life products. Defendants advertises living benefits that purportedly grant access to death benefits for individuals facing terminal, chronic, or critical illnesses. In addition, Defendants promote retirement planning solutions, such as annuities, and college savings plans, claiming to help families achieve their financial goals. In providing these services Defendants solicited and required Plaintiff and Class Members to surrender their personally identifiably information ("PII") and protected health information ("PHI").

3. On or about October 17, 2023, due to Defendant's failure to provide reasonable safeguards to protect Plaintiff's and Class Members' PII/PHI cybercriminals accessed and exfiltrated Plaintiff's and Class Members' PII/PHI (the "Data Breach"). The cybercriminals accessed and stole Plaintiff's and Class Members' names, **social**

security numbers, addresses, dates of birth, medical information, and phone numbers.

4. Defendants disclosed the data breach to Plaintiff and Class Members on January 19, 2024 (the "Data Breach Notice"). However, Defendants failed to reveal when it first became aware of the Data Breach, stating only that an investigation involving outside IT experts commenced on November 28, 2023—more than a month after the breach.

5. Despite noticing and confirming the criminal activity as early as November 28, 2023, Defendants failed to inform Class Members that their PII/PHI had been accessed and exfiltrated until January 19, 2024, more than 90 days after the Data Breach first occurred. Defendants have not disclosed the number of additional members and clients believed to be impacted by the Data Breach.

6. Across multiple states, hundreds of thousands of clients sought out and/or used Defendants' services to obtain services, and hackers stole, viewed, and used their highly sensitive PII/PHI, including Social Security Numbers, without the victims' knowledge. Defendant's lax security practices allowed this intrusion to occur. Their failure to promptly notify Plaintiff and Class Members about the Data Breach has worsened Plaintiff's and other Class Members' lives by, among other injuries: (a) adding to their already heightened financial obligations by placing them at a significantly increased risk of fraud; (b) a significantly increased risk of identity theft; and/or (c) increasing the risk of other potential personal, professional, or financial harms that could be caused as a result of having their PII/PHI exposed.

7. Before the Data Breach, Defendants acknowledged in their confidentiality and privacy policy that the policy's purpose was to ensure the privacy of PII/PHI complied with local, state, and federal laws, rules, and regulations which govern the release of PII and PHI. Defendants' policy recognized and protected the right of privacy as outlined in local, state, and federal laws, rules, and regulations. Defendants not only promised and led their clients to believe their PII/PHI would be kept safe, but Defendants failed to live up to their duties and obligations as required by law and

industry standards.

8. Defendants were required to provide notice of information practices concerning insurance transactions to Plaintiff and Class Members, as mandated by law ("Privacy Policies"). This notice was delivered at three key points: (1) upon delivery of the insurance policy or certificate when personal information had been collected; (2) before or on the date of policy renewal or confirmation; and (3) upon requests for policy reinstatement or changes to insurance benefits. The notice outlined Defendants' practices regarding the collection, retention, and disclosure of Plaintiff's and Class Members' PII/PHI, including whether information might be collected from third parties, the types and sources of information collected, and circumstances under which disclosure could occur without authorization. It also informed recipients of their rights under Insurance Code §§ 791.08 and 791.09, how to exercise those rights and the practices of insurance-support organizations. Additionally, Defendants were required to disclose their confidentiality and security policies for nonpublic personal information, including a general description of who is authorized to access it, in accordance with Insurance Code § 791.045(a)(1)-(2) and Cal. Code Regs., tit. 10, § 2689.7.

9. Had Defendants revealed that they utilized inadequate security measures—including data security practices at odds with their affirmative representations—Plaintiff and other Class Members would have been unwilling to sign up or pay for Defendants' services at the prices charged, would not have used Defendants' services at all and/or been unwilling to provide their PII/PHI to Defendants.

10. Contrary to their promises to help clients improve the quality of their lives, Defendants' conduct has, instead, been a direct cause of the ongoing harm to Plaintiff and other Class Members whose suffering has been magnified by both the Data Breach and Defendants' delayed notification of the Data Breach, and who will continue to experience harm and data insecurity for the indefinite future. Defendants' failure to implement adequate security protocols jeopardized hundreds of thousands of its

members' PII/PHI, fell well short of their legal obligations and industry standards, fell well short of Plaintiff's and Class Members' reasonable expectations when they provided their PII/PHI to Defendants, and has diminished the value of Defendants services.

11. Specifically, Defendants failed to maintain reasonable and/or adequate security measures to protect Plaintiff's and other Class Members' PII/PHI from unauthorized access and disclosure, apparently lacking, at a minimum: (1) reasonable and adequate security measures designed to prevent this attack, even though Defendants knew or should have known that it was a prized target for hackers; and (2) reasonable and adequate security protocols to promptly detect the unauthorized intrusion into and removal of PII/PHI from their network.

12. As Defendants undoubtedly knew, armed with PII/PHI, hackers can sell the PII/PHI to other unauthorized users or misuse it themselves to commit a variety of crimes that could and did harm Plaintiff and Class Members. For instance, hackers can take out loans, mortgage property, open financial accounts and/or open credit cards in a victim's name, use a victim's information to obtain government benefits or file fraudulent returns to obtain a tax refund, obtain a driver's license or identification card in a victim's name, gain employment in another person's name, give false information to police during an arrest, or engage in medical fraud that can result in financial harm or a harmful misdiagnosis to Plaintiff and Class Members.

13. As a result of Defendants' willful failure to prevent the Data Breach and its reckless and negligent disclosure of Plaintiff's and Class Members' PII/PHI, Plaintiff and Class Members are more susceptible to identity theft, fraud, and other harm, and have experienced, will continue to experience, and face an increased risk of financial harms.

PARTIES

14. Plaintiff Yvette Price is a resident citizen of the State of California. Plaintiff Price is a client of Defendants and otherwise received services from

Defendants. In exchange for these services, Plaintiff Price provided her PII/PHI to Defendants with the understanding and expectation that Defendants would adequately safeguard her PII/PHI. Plaintiff Price believed, at the time of receiving services from Defendants, that they would maintain the privacy and security of her PII/PHI. Plaintiff Price further believes she paid a premium to Defendants for their data security, and he would not have used Defendants' services or provided her PII/PHI to Defendants had he known that they would expose, or allow to be exposed, her PII/PHI, making it available to unauthorized parties. On or about January 19, 2023, Defendants sent Plaintiff Price a Data Breach Notice, which indicated that her PII/PHI, including Social Security Number, had been acquired by unauthorized parties during the Data Breach. These unauthorized parties accessed, viewed and exfiltrated Plaintiff Price's PII/PHI. The Data Breach and Defendants' actions, injured Plaintiff Price, suffered financial losses, and is subject to a substantial risk for further identity theft due to Defendants' Data Breach.

15. Defendant First Financial Security, Inc. is a Delaware corporation with its principal place of business at 11695 Johns Creek Pkwy Johns Creek, GA 30097. Defendant collects PHI as part of its life insurance services and death benefits for individuals facing terminal, chronic, or critical.

16. The true names and/or capacities, whether individual, corporate, partnership, associate or otherwise, of the Defendants herein designated as Does 1 to 50 are unknown to or presently being investigated by Plaintiff at this time, and Plaintiffs, therefore, sue said Defendants by fictitious names. Plaintiff alleges that each named Defendant herein designated as a Doe party is negligently, willfully or otherwise legally responsible for the events and happenings herein referred to and proximately caused damages to Plaintiffs, as herein alleged. Plaintiff will seek leave of Court to amend this Complaint to insert the true names and capacities of such Defendants when they have been ascertained and will further seek leave to join said Defendants in these proceedings.

17. The true names and/or capacities, whether individual, corporate, partnership, associate or otherwise, of the Defendants herein designated as Does 51 to 100 are unknown to or presently being investigated by Plaintiff at this time, and Plaintiffs, therefore, sue said Defendants by fictitious names. Plaintiff alleges that each named Defendant herein designated as a Doe party negligently entrusted Plaintiff's and Class Members' PII/PHI to the other Defendants or is otherwise legally responsible for the events and happenings herein referred to and proximately caused damages to Plaintiffs, as herein alleged. Plaintiff will seek leave of Court to amend this Complaint to insert the true names and capacities of such Defendants when they have been ascertained and will further seek leave to join said Defendants in these proceedings.

18. Doe parties were agents, servants, employees, partners, distributors, joint ventures, Business Associates under IIPPA of each other, and/or otherwise entrusted Defendants with Plaintiff's and Class Members' PII/PHI and that, in doing the acts herein alleged, were acting within the course and scope of said agency, employment, partnership joint venture or Business Associate relationship. Each and every aforesaid Defendant was acting as a principal and was negligent or grossly negligent in the selection, hiring and training of each and every other Defendant, ratified the conduct of every other Defendant as an agent, servant, employee, joint venture, or Business Associate, or otherwise negligently entrusted Plaintiff's and Class Members' PII/PHI to one another.

19. Each of the Defendants was and is an agent of the other Defendants. Each Defendant, in acting or omitting to act as alleged in this Complaint, was acting in the course and scope of its actual or apparent authority pursuant to such agencies, and/or the alleged acts or omissions of each Defendant as an agent were subsequently ratified and adopted by each agent as a principal. Each Defendant, in acting or omitting to act as alleged in this Complaint, was acting through its agents, and is liable based on the acts and omissions of its agents.

20. There existed a unity of interest in ownership between all Defendants such

that the individuality and separateness between them ceased where they were the alter ego of one another, in that, among other things, Defendants controlled, dominated, managed, and operated the other Defendants as their alter egos. The vast majority of the IIPPA Policies and Procedures found on Defendants' and other Defendants' websites are policies and procedures that were prepared and applied to all clients of all Defendants.

21. Defendants should have, would have, and did perform cybersecurity due diligence before any affiliation with the other Defendants, consistent with industry standards, which would include researching undisclosed or unknown data breaches, as well as identifying information technology ("IT") security risks and shortfalls in operations and governance of the target company, the results of which should have or would have been shared with all Defendants.

22. Defendants performed or required the other Defendants to perform a full and complete cyber-security assessment before and because of the affiliation between the Defendants, to understand the state of the other Defendants' computer networks/systems and/or any shared networks/systems between Defendants, including their vulnerabilities. The results of these assessments would have been shared between the Defendants.

23. Defendants, each of them, could have, would have, and did retain respective financial advisors and legal counsel to analyze business records and make a financial assessment of the affiliation with the other Defendants, which would have or should have included retaining a cybersecurity analyst to audit the other Defendants' information security risks and shortfalls, IT operations, technology, and governance, the results of which would have been shared with Defendants.

24. Defendants, each of them, either failed to engage in the above-described due diligence or failed to take appropriate and necessary measures because of the due diligence that would have protected the PII/PHI of Plaintiff and Class Members.

25. Defendants intentionally, willfully, recklessly, or negligently failed to take

adequate and reasonable measures to ensure its and other Defendants' data systems and/or any shared networks were protected against unauthorized intrusions.

JURISDICTION AND VENUE

26. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. Plaintiffs and Defendants are citizens of different states. And there are over 100 putative Class Members. There is minimal diversity.

27. This Court has personal jurisdiction over Defendants because Defendants have sufficient contacts with the forum state such that maintenance of the lawsuit does not offend "traditional notions of fair play and substantial justice." *International Shoe Co. v. Washington*, 326 U.S. 310 (1945).

28. Venue is appropriate in this Court because substantial events occurred in this district and Defendant is subject to personal jurisdiction with respect to the action.

FACTUAL ALLEGATIONS

The Data Breach

29. On or about October 17, 2023, unauthorized parties accessed Defendants' network that contained Plaintiff's and Class Members' PII/PHI. Plaintiff and Class Members are clients who paid and provided their PII/PHI directly or indirectly to Defendants in exchange for services.

30. For more than a week, unauthorized parties maintained uninterrupted access to Defendants' servers containing the PII/PHI of hundreds of thousands of clients. Between October 17, 2023, and sometime before November 28, 2022, unauthorized parties accessed, viewed, stole Plaintiff's and Class Members' PII/PHI, and installed malicious software and exfiltrated files which contained Plaintiff's and Class Members' PII/PHI.

31. Defendants consciously disregarded the rights of Plaintiff and Class Members amounting to malice and/or willful intent, Civil Code § 3294, because

Defendants' inadequate data security measures were brought to Defendants' attention before the Data Breach and Defendant, knowing that it possessed the PII/PHI of Plaintiff and Class Members and their rights regarding the privacy and confidentiality of their PII/PHI intentionally ignored the warnings for profit motive reasons.

32. Motivated by pecuniary self-interests, Defendants intentionally failed to monitor its data systems continuously and run security audits; Defendants failed to implement multi-factor authentication for the employee and agent user accounts involved in the breach, allowing unauthorized access to PII/PHI and demonstrating a failure to adopt reasonable security measures. Defendants improperly granted excessive privileges to standard employee accounts, which allowed bad actors with access to use standard employee accounts to compromise other accounts within the system, supercharging their reach and the system's vulnerability. Further, Defendants designed their network in a manner that allowed compromised accounts to move laterally across the environment, permitting unauthorized access through PowerShell commands. Additionally, Defendants established a two-way trust relationship between their respective Active Directory domains, which facilitated the unauthorized sharing of Private Information across domains and further compromised system integrity. These failures were compounded by weak password practices, lack of employee training, unpatched vulnerabilities, poor access controls, inadequate data encryption, neglect of system updates, susceptibility to social engineering attacks and phishing scams, insider threats, and insufficient monitoring. Thus, Defendants consciously disregarded the rights of Plaintiff and Class Members.

33. Although Defendants became aware of the Data Breach on October 17, 2023, Defendants failed to inform Plaintiff and Class Members of the Data Breach until approximately January 18, 2024, more than two months after unauthorized parties first accessed Defendants' systems and nearly two months after Defendants allegedly detected the Data Breach.

34. In their Notice of Data Breach, Defendants provided the following

description of what happened with respect to the Data Breach:

> On October 17, 2023, FPS was the victim of a ransomware attack which our data protection team discovered was an attempt to access and freeze all of our Information Systems Data. This included both sensitive and non-sensitive data. Thankfully the ransom ware attack was not successful in freezing our systems and disrupting our operations. With the help of outside IT security experts, we have determined that a very limited amount of system data was exposed. We were able to determine on November 28, 2023, the specific data that was exposed.

35. With respect to what information was involved in the Data Breach, Defendants provided the following description:

> We are providing you this notification in an abundance of caution in case someone actually viewed or had access to your information that would have included your full name, personal information, social security number.

36. With respect to what actions Defendants were taking at that time in response to the Data Breach, Defendants provided the following information:

> We have secured the services of IDX, A ZeroFox Company and data breach and recovery services expert, to provide call center services and to provide identity monitoring at no cost to you. IDX identity protection services include: 12 months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

37. With respect to what steps Defendants recommended Plaintiff and Class Members take in response to the Data Breach, Defendants provided the following information:

> We encourage you to contact IDX with any questions and to enroll in the free identity protection services by calling 1-888-927-7176, going to https://app.idx.us/account-creation/protect, or scanning the QR image and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9 am - 9 pm Eastern Time. Please note the deadline to enroll is April 19, 2024.

Thus, even Defendants acknowledge the risks associated with the Data Breach and that Plaintiff and Class Members should take immediate steps to protect themselves from

potential harm, including registering for identity protection services. Defendants are, thus, estopped from contending Plaintiff's and Class Members' protective actions were unnecessary, unwise, or unwarranted.

Defendants Promised to Protect Plaintiff's and Class Members' PII/PHI

38. Defendants require that their clients provide highly sensitive PHI and PII as a condition of receiving services. In the ordinary course of receiving services, clients must provide sensitive personal and private information, such as the PII/PHI disclosed in the Data Breach.

39. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' PII/PHI, Defendants assumed legal and equitable duties and knew or should have known they were responsible for protecting Plaintiff's and Class Members' PII/PHI from disclosure.

40. Defendants made numerous promises to Plaintiff and Class Members that they would maintain the security and privacy of their PII/PHI. For instance, in the privacy policies and statements made by Defendants represented that Defendants ensured the privacy of PII/PHI in compliance with local, state, and federal laws, rules, and regulations which govern the release of PII/PHI. Defendants further promised that its recognized and protected the right of privacy as set forth in the IIPPA Privacy Standards and the Confidentiality of Medical Information Act, which govern the release of patient-identifiable information.

41. In addition, Defendants stated clients have the right to expect that all communications and other records pertaining to their services and payments will be treated as confidential.

42. Defendants provided each of their clients with a copy of their privacy policies and Plaintiff and Class Members read, understood, acknowledged and agreed to surrender their PII/PHI in as a condition of receiving Defendants' services. As a result of Plaintiff and Class Members agreeing to surrender, Defendants provided services with the understanding that they were obligated to protected Plaintiff and Class

Members' PII/PHI as promised.

43. Through these policies, among others, Defendants made promises to Plaintiff and Class Members that they would protect their PII/PHI by maintaining adequate data security, acknowledged that they were a predictable target of unauthorized parties for a data breach, such as the Data Breach, and led Plaintiff and Class Members to believe Defendants could be trusted with their PII/PHI. Defendants broke these privacy promises by failing to protect Plaintiff's and Class Members' PII/PHI by allowing the Data Breach to occur and otherwise disclosing Plaintiff's and Class Members' PII/PHI.

44. Plaintiff and Class Members took reasonable steps to maintain the confidentiality of their PII/PHI and relied on Defendants to keep their PII/PHI confidential and securely maintained.

45. Had Plaintiff and Class Members known the truth about Defendants' inadequate data security, they would not have surrendered their PII/PHI to Defendants.

Personally Identifiable Information/Protected Health Information

46. PII/PHI is of great value to hackers and cyber criminals, and the data compromised in the Data Breach can be used in a variety of unlawful manners.

47. PII/PHI is information that can be used to distinguish, identify, or trace an individual's identity, *inter alia*: Social Security number, biometric records. This identification can be accomplished alone or in combination with other personal or identifying information that is connected or linked to an individual, such as birthdate, birthplace, and mother's maiden name.

48. PII/PHI exceeds data that can be used to directly identify or contact an individual (*e.g.*, name, address, and phone number) or personal data that is especially sensitive (*e.g.*, Social Security number, diagnosis and treatment information, laboratory test results, prescription data, radiology reports, Medicare ID number, and health plan member number).

49. PHI—like the type disclosed in the breach—is particularly valuable for

cybercriminals. According to the Ponemon Institute and Verizon Data Breach Investigations Report, the health care industry experiences more data breaches than any other sector.[1] While regular PII can be sold at a price ranging from $40 to $200, and bank details sold at a price range of $50 to $200,[2] PHI can sell for as much as $363, according to the Infosec Institute.[3] This is because one's personal health history cannot be changed, unlike more dynamic information such as credit card numbers and security codes.

50. The insurance industry is a well-known target to hackers.[4] In 2023 alone, multiple insurance companies became victims of significant cyberattacks, including the widespread MOVEit file transfer breach. Notable targets included Sun Life in June through an attack on its vendor Pension Benefits Information LLC, Prudential Insurance in May, which impacted more than 320,000 customer accounts, and New York Life Insurance Company, which had 25,700 accounts affected during the same period as the Prudential breach. Genworth Financial faced one of the largest impacts, with up to 2.7 million individuals affected. Beyond MOVEit, other ransomware attacks also hit the industry. In April, Point32Health, the parent company of Harvard Pilgrim Health Care and Tufts Health Plan, suffered a ransomware breach, while NationsBenefits reported being targeted by the Cl0p ransomware gang. The most extensive attack occurred when Managed Care of North America Dental, an insurer, experienced a LockBit attack that compromised data for 9 million patients.

51. The insurance industry's growing vulnerability stems from its rapid migration to digital platforms, as highlighted by consulting firm Deloitte. This digital

---

[1] Center for Internet Security, *Data Breaches: In the Healthcare Sector*, <https://www.cisecurity.org/insights/blog/data-breaches-in-the-healthcare-sector> [as of August 4, 2023].

[2] Digital Trends, *Your personal data is for sale on the dark web. Here's how much it costs,* (Oct. 16, 2019), <https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/> [as of August 4, 2023].

[3] Center for Internet Security, *Data Breaches: In the Healthcare Sector*, <https://www.cisecurity.org/insights/blog/data-breaches-in-the-healthcare-sector> [as of August 4, 2023].

[4] https://www.darkreading.com/cyber-risk/insurance-companies-have-a-lot-to-lose-in-cyberattacks. [as of December 19, 2024].

transformation, aimed at strengthening customer relationships and expanding service portfolios, has spurred increased investment in core IT systems, agency portals, and mobile-based applications. However, this shift also exposes insurers to heightened cyber risks. Deloitte observed that as insurers innovate in analyzing and managing customer data, they must prioritize securing this data against cyber threats. The wealth of personal and corporate data within the insurance sector makes it a lucrative target for attackers, with insurance applications often revealing sensitive details about customers and companies. Authorities are also aware of the problem. For instance, the Wall Street Journal reported on November 25, 2024, that New York State fined Geico and Travelers $11.3 Million for Data Breaches. [5] The penalties arose from a series of cyberattacks that targeted Geico's auto insurance quoting tools in late 2020 and a similar Travelers tool in early 2021. New York officials found that Geico failed to adequately safeguard prospective customers' driver's license numbers within its internal systems.

52. Insurance applications are a particular concern due to their volume of critical data. According to Marc Schein, national co-chair of the Cyber Risk Practice at Marsh McLennan Agency, these applications often expose information about the level of insurance coverage a company has, which ransomware attackers can exploit to maximize ransom demands. Additionally, applications can reveal weaknesses in a company's network security, while other policies, such as errors and omissions or directors' and officers' coverage, may expose trade secrets and private executive data. Patricia Titus, chief privacy and information security officer at Markel Insurance, further noted that applications often highlight "technology debt," such as unpatched software, outdated hardware, and legacy systems, all of which could represent exploitable vulnerabilities for attackers.

53. Because Defendant offers life insurance and similar products, the Defendants possess the PII/PHI of its clients. Cybercriminals know of the high value of PHI as shown by their attacks on the healthcare industry which experienced a large and

[5] https://www.wsj.com/articles/new-york-state-fines-geico-and-travelers-11-3-million-for-data-breaches-fb7218a3? [as of December 19, 2024]

growing number of high-profile cyberattacks. Indeed, an analysis of data breaches recorded on the Privacy Rights Clearinghouse database between 2015 and 2019 showed that 76.59% of all recorded data breaches were in the healthcare sector. This implies the healthcare sector recorded three times as many data breaches as the education, finance, retail, and government sectors combined.[6]

54. According to analysis performed by U.S. Department of Health and Human Services ("HHS"), 45 million people in 2021 were affected by healthcare cyberattacks, triple the 14 million affected in 2018.[7] In 2022, HHS posted an alert warning healthcare organizations of an "exceptionally aggressive" ransomware group that is known to target the healthcare center and noted that healthcare organizations should try to protect themselves with continuous monitoring and an active vulnerability management program.[8] The alert also suggested keeping backups of data in multiple locations and using two-factor authentication with strong passwords.

55. According to a TENABLE study conducted over a 14-month period, a "root cause was reported in 93.17% of the healthcare breaches disclosed in the 14-month period [it] analyzed. Among these, ransomware was by far the most prominent root cause of healthcare breaches, accounting for a whopping 54.95%. Other leading causes included email compromise/phishing (21.16%), insider threat (7.17%) and unsecured databases (3.75%)."[9]

56. In a survey released by Ponemon Institute in January 2023, nearly half of respondents (47%) said their organizations experienced a ransomware attack in the past two years, up from 43% in 2021. 45% of those respondents reported complications from

---

[6] HIPAA Journal, *Healthcare Data Breach Statistics*, <https://www.hipaajournal.com/healthcare-data-breach-statistics/>, [as of August 4, 2023].

[7] Healthcare Dive, *Tenet says 'cybersecurity incident' disrupted hospital operations*, <https://www.healthcaredive.com/news/tenet-says-cybersecurity-incident-disrupted-hospital-operations/622692/> [as of August 4, 2023].

[8] Healthcare Dive, *HHS warns providers of 'exceptionally aggressive' ransomware group*, < https://www.healthcaredive.com/news/hhs-warns-providers-of-exceptionally-aggressive-ransomware-group/622470/> [as of August 4, 2023].

[9] TENABLE, *Root Cause Analysis of Healthcare Breaches*, < https://www.tenable.com/blog/healthcare-security-ransomware-plays-a-prominent-role-in-covid-19-era-breaches>, [as of August 4, 2023].

medical procedures due to ransomware attacks, up from 36% in 2021.[10]

57. In light of several recent high profile cybersecurity incidents affecting the healthcare industry, including the American Medical Collection Agency (25 million patients, March 2019), University of Washington Medicine (974,000 patients, December 2018), Florida Orthopedic Institute (640,000 patients, July 2020), Wolverine Solutions Group (600,000 patients, September 2018), Oregon Department of Human Services (645,000 patients, March 2019), Elite Emergency Physicians (550,000 patients, June 2020), Magellan Health (365,000 patients, April 2020), and BJC Health System (286,876 patients, March 2020), Defendants knew or should have known that their electronic records would be targeted by cybercriminals.

58. Given the nature of the Data Breach, it is foreseeable that the compromised PII/PHI will be used to access Plaintiff's and the Class Members' other accounts, thereby providing access to additional PII/PHI or personal and sensitive information. Therefore, the compromised PII/PHI in the Data Breach is of great value to hackers and unauthorized users and can be used in a variety of ways. Information about, or related to, an individual for which there is a possibility of logical association with other information is of great value to hackers and unauthorized users. Indeed, "significant evidence demonstrates that technological advances and the ability to combine disparate pieces of data can lead to the identification of a consumer, computer or device even if the individual pieces of data do not constitute PII."[11] For example, different PII/PHI elements from various sources may be linked to identify an individual or access additional information about or relating to that individual.

59. Further, as technology advances, computer programs may scan the Internet with an ever-widening scope to create a mosaic of information that may be used to link

[10] Chief Healthcare Executive, California medical group discloses ransomware attack, more than 3 million affected, <https://www.chiefhealthcareexecutive.com/view/california-medical-group-discloses-ransomware-attack-more-than-3-million-affected>, [as of August 4, 2023].

[11] Fed. Trade Comm'n, Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers, Preliminary FTC Staff Report 35-38 (Dec. 2010) <https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-bureau-consumer-protection-preliminary-ftc-staff-report-protecting-consumer/101201privacyreport.pdf> [as of August 4, 2023].

information to an individual in ways not previously possible. This is known as the "mosaic effect."[12]

60. Names and dates of birth, combined with contact information like telephone numbers and addresses, are very valuable to hackers and identity thieves as these items allow them to access users' other accounts, particularly when those users have easily decrypted passwords or security questions.

61. The PII/PHI that Defendants exposed is of great value to hackers and cyber criminals, and the data compromised in the Data Breach can be used in a variety of unlawful manners, including opening new credit and financial accounts in victims' names, obtaining protected health information, and/or committing medical fraud.

62. Unfortunately, for Plaintiff and Class Members, a person whose PII/PHI has been compromised may not fully experience the effects of the breach for years to come:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[13]

63. Accordingly, Plaintiff and Class Members will bear a heightened risk of injury for years to come. Identity theft is one such risk and occurs when an individuals' PII/PHI is used without his or her permission to commit fraud or other crimes.

64. According to the Federal Trade Commission, "the range of privacy-related harms is more expansive than economic or physical harm or unwarranted intrusions and that any privacy framework should recognize additional harms that might arise from

[12] Fed. Chief Information Officers Council, Recommendations for Standardized Implementation of Digital Privacy Controls (Dec. 2012) pp. 7-8.

[13] G.A.O., Personal Information: Data Breaches are Frequent, but Evidence of Resulting Identity Theft is Limited; However, the Full Extent is Unknown (June 2007) <https://www.gao.gov/assets/gao-07-737.pdf.> [as of August 4, 2023].

unanticipated uses of data."[14]

IIPPA Provides Standards For How Defendants Must Secure Clients' PII/PHI

65. The California Insurance Information and Privacy Protection Act ("IIPPA") establishes strict privacy standards for the collection, use, and disclosure of personal information by insurance companies, agents, and insurance-support organizations (Cal. Ins. Code §§ 791 to 791.29). Under IIPPA, insurance entities are generally prohibited from disclosing personal information collected or received during an insurance transaction without the individual's authorization, unless the disclosure is necessary for conducting legitimate business purposes (Cal. Ins. Code § 791.13). Additionally, IIPPA mandates that insurance entities provide applicants and policyholders the opportunity to opt out of any disclosures made for marketing purposes (Cal. Ins. Code § 791.13(k)).

66. IIPPA further requires insurance entities to issue a privacy notice to applicants and policyholders that clearly outlines their information practices. This notice must describe the types of personal information collected, the methods and sources of collection, the purposes for which information may be disclosed, and the conditions under which disclosure may occur without authorization. It must also detail individuals' rights under IIPPA, including the right to access and correct personal information, as well as the procedures for exercising these rights (Cal. Ins. Code §§ 791.08, 791.09). The privacy notice must also address the company's policies for safeguarding nonpublic personal information, specifying who is authorized to access such information and the measures in place to ensure its confidentiality and security (Cal. Ins. Code § 791.045; Cal. Code Regs., tit. 10, § 2689.7).

67. California safeguards residents' personal information under the California Consumer Privacy Act of 2018 (CCPA), as amended by the California Privacy Rights Act of 2020 (CPRA) (Cal. Civ. Code §§ 1798.100–1798.199.100; Cal. Code Regs. Tit.

[14] Fed. Trade Comm'n, Protecting Consumer Privacy in an Era of Rapid Change (March 2012) <https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf> [as of August 4, 2023].

11, §§ 7000–7304). The CCPA grants residents several key rights concerning their personal information.

68. The CCPA requires businesses to assess their data collection, sharing, and processing practices to determine compliance obligations, especially if they sell, share, or handle sensitive personal information. Even businesses that do not engage in these activities must implement clear internal processes to comply with use restrictions and respond to consumer requests effectively.

69. Under the CCPA, covered businesses must implement reasonable security procedures and practices appropriate to the nature of the personal information they handle, ensuring protection against unauthorized access, use, modification, disclosure, or destruction (Cal. Civ. Code § 1798.100(e)). These requirements align with California's data security safeguards law (Cal. Civ. Code § 1798.81.5(a)) and emphasize the need for robust security measures. The CCPA defines "security and integrity" to include:

a. The ability of networks or information systems to detect and respond to security incidents that compromise the availability, authenticity, integrity, and confidentiality of stored or transmitted personal information.

b. A business's capacity to identify security threats, resist malicious or fraudulent actions, and assist in prosecuting those responsible.

c. Ensuring the physical safety of individuals (Cal. Civ. Code § 1798.140(ac)).

70. Additionally, the CCPA provides a private right of action for consumers affected by data breaches that result from a business's failure to implement and maintain reasonable security measures appropriate to the level of risk (Cal. Civ. Code § 1798.150(a)(1)).

Other Federal and State Laws and Regulations Existed to Guide Defendants' Conduct

71. Section 5(a) of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. §

45, prevents Defendants from using "unfair or deceptive acts or practices in or affecting commerce." The FTC has found that inadequate data privacy and cybersecurity practices can constitute unfair or deceptive practices that violate § 5.

72. In addition to their obligations under federal and state laws and regulations, Defendants owed a common law duty to Plaintiff and Class Members to protect PII/PHI entrusted to them, including to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII/PHI in their possession from being compromised, lost, stolen, accessed, viewed, and misused by unauthorized parties.

73. Defendants further owed and breached their duty to Plaintiff and the Class to implement processes and specifications that would detect a breach of their security systems in a timely manner and to timely act upon warnings and alerts, including those generated by their own security systems (e.g., 45 CFR §§ 164.308(a), 164.306(d), 164.312, The Office for Civil Rights July 14, 2010 Guidance on Risk Analysis Requirements under the HIPAA Security Rule, etc.).

74. As a direct and proximate result of Defendants' reckless and negligent actions, inaction, and omissions, the resulting Data Breach, the unauthorized release and disclosure of Plaintiff's and Class Members' PII/PHI, and Defendants' failure to properly and timely notify Plaintiff and Class Members, Plaintiff and Class Members are more susceptible to identity theft and have experienced, will continue to experience and will face an increased risk of experiencing the following injuries, *inter alia*:

d. money and time expended to prevent, detect, contest, and repair identity theft, fraud, medical fraud, and/or other unauthorized uses of personal information;

e. money and time lost because of fraudulent access to and use of their accounts, including financial accounts;

f. loss of use of and access to their financial accounts and/or credit;

g. money and time expended to avail themselves of assets and/or credit

frozen or flagged due to misuse;

h. impairment of their credit scores, ability to borrow, and/or ability to obtain credit;

i. lowered credit scores resulting from credit inquiries following fraudulent activities;

j. money, including fees charged in some states, and time spent placing fraud alerts and security freezes on their credit records;

k. costs and lost time obtaining credit reports to monitor their credit records;

l. anticipated future costs from the purchase of credit monitoring and/or identity theft protection services;

m. costs and lost time from dealing with administrative consequences of the Data Breach, including by identifying, disputing, and seeking reimbursement for fraudulent activity, canceling compromised financial accounts and associated payment cards, and investigating options for credit monitoring and identity theft protection services;

n. money and time expended to ameliorate the consequences of the filing of fraudulent tax returns;

o. lost opportunity costs and loss of productivity from efforts to mitigate and address the adverse effects of the Data Breach including, but not limited to, efforts to research how to prevent, detect, contest, and recover from misuse of their personal information;

p. loss of the opportunity to control how their PII/PHI is used; and

q. continuing risks to their personal information, which remains subject to further harmful exposure and theft as long as Defendants fail to undertake appropriate, legally required steps to protect the personal information in its possession.

75. The risks associated with identity theft are serious. "While some identity theft victims can resolve their problems quickly, others spend hundreds of dollars and

many days repairing damage to their good name and credit record. Some consumers victimized by identity theft may lose out on job opportunities or be denied loans for education, housing, or cars because of negative information on their credit reports. In rare cases, they may even be arrested for crimes they did not commit."[15]

76. Further, criminals often trade stolen PII/PHI on the "cyber black-market" for years following a breach. Cybercriminals can post stolen PII/PHI on the internet, making such information publicly available.

77. HIPAA as guidance. Defendants are not entities subject to the HIPAA Privacy Rule ("Standards for Privacy of Individually Identifiable Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and E, and the HIPAA Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C (collectively, "Privacy and Security Rules"). However, the HIPAA guidelines inform Defendants' standard of care in handling and safeguarding Plaintiff's and Class Members' PHI. Further, because Defendants Life Insurance and other related products routinely require and analyze medical information, Defendants know the HIPAA standards. Defendants must adhere to the privacy and confidentiality requirements that apply to the medical information they receive from covered entities.

78. The Privacy and Security Rules establish a national set of standards for protecting "individually identifiable health information" that is held or transmitted by a health care provider or health care service plan, which HIPAA refers to as "protected health information."

79. Pursuant to HIPAA, Defendants must maintain reasonable and appropriate administrative, technical, and physical safeguards for protecting PHI.

80. HIPAA imposes general security standards that Defendants must follow, including:

a. Ensuring the confidentiality, integrity, and availability of all

[15] *South Dakota Consumer Protection, Identity Theft,* <https://consumer.sd.gov/fastfacts/identitytheft.aspx> [as of Aug. 4, 2023].

electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits, 45 C.F.R. § 164.306(a);

b. Protecting against any reasonably anticipated threats or hazards to the security or integrity of such information, 45 C.F.R. § 164.306(a);

c. Protecting against any reasonably anticipated uses or disclosures of such information that are not permitted or required under HIPAA, 45 C.F.R. § 164.306(a); and

d. Reviewing and modifying the security measures implemented under HIPAA as needed to continue provision of reasonable and appropriate protection of electronic protected health information, 45 C.F.R. § 164.306(e).

81. From a technical standpoint, HIPAA requires Defendants to, among other things:

a. Implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights, 45 C.F.R. § 164.312(a);

b. Implement procedures to verify that a person or entity seeking access to electronic PHI is the one claimed, 45 C.F.R. § 164.312(d); and

c. Implement technical security measures to guard against unauthorized access to electronic PHI that is being transmitted over an electronic communications network, 45 C.F.R. § 164.312(e).

82. The HIPAA Security Rule requires implementation of reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of the HIPAA Security Rule. 45 CFR 164.316(a). These policies and procedures must be maintained in written form. 45 CFR 164.316(b)(1)(i).

83. The HIPAA Security Rule requires covered entities to maintain a written record of any action, activity, or assessment required to be documented by the HIPAA Security Rule. 45 CFR 164.316(b)(1)(ii).

84. The HIPAA Security Rule requires covered entities to review documentation periodically and update it as needed, in response to environmental or operational changes affecting the security of the electronic protected health information. 45 CFR 164.316(b)(1)(iii).

85. Under the HIPAA Privacy Rule, use or disclosure of PHI or confidential medical information is prohibited except as expressly permitted. 45 CFR 164.502(a).

CLASS ACTION ALLEGATIONS

86. Plaintiff intends to seek certification of a Nationwide Class and a California subclass. Plaintiff brings this class action under Fed. R. Civ. P. 23(a), 23(b)(2), and 23(b)(3), individually and on behalf of all members of the Class is initially defined as follows:

> Nationwide Class: All individuals whose PII/PHI was compromised in the Data Breach announced by Defendants.
>
> California Subclass: All persons residing in California whose PII/PHI was compromised in the Data Breach announced by Defendants.

87. The scope of these class definitions may be further refined after discovery of Defendants' and/or third-party records.

88. Excluded from the Classes are governmental entities, Defendants, any entity in which Defendants have a controlling interest, and Defendants' officers, directors, affiliates, legal representatives, co-conspirators, successors, subsidiaries, and assigns. Also excluded from the Classes are any judge, justice, or judicial officer presiding over this matter and the members of their immediate families and judicial staff.

89. Plaintiff's claims are typical of the claims of the Class. Plaintiff is a member of a well-defined Class of similarly situated persons and the members of the Class were similarly affected by the conduct alleged of Defendants and incurred similar damage, as alleged in this complaint, because of the conduct of Defendants. Members of the Class are ascertainable from Plaintiff's description of the Class and/or

Defendants' records and/or records of third parties accessible through discovery.

90. The representative Plaintiff will fairly and adequately represent the members of the Class and have no interests which are antagonistic to the claims of the Class. Plaintiff's interests in this action are antagonistic to the interests of Defendants, and Plaintiff will vigorously pursue the claims of the Class.

91. The representative Plaintiff has retained counsel who are competent and experienced in consumer, data breach, and invasion of privacy class action litigation, and have successfully represented Plaintiff in complex class actions. Plaintiff's counsel currently represents other Plaintiff in similar complex class action litigation involving wrongful disclosures and access of PII/PHI.

92. Common questions of law and fact impact the rights of each member of the Class and a common remedy by way of permissible damages and/or injunctive relief is sought for the Class.

93. There are substantial questions of law and fact common to all members of the Class which will predominate over any individual issues. These common questions of law and fact include, without limitation:

a. Whether Defendants disclosed the PII/PHI of Plaintiff and the Class, without authorization;

b. Whether such conduct constitutes a violation of California Insurance Code, § 791.01, *et seq*.;

c. Whether Defendants timely notified the clients whose information was wrongly disclosed;

d. Whether Defendants' notice was deficient;

e. Whether Defendants' conduct was negligent;

f. Whether Defendants knew or should have known that their data security systems, policies, procedures, and practices were vulnerable;

g. Whether Plaintiff and Class Members suffered legally cognizable

damages because of Defendants' conduct, including increased risk of identity theft and loss of value of PII/PHI;

h. Whether Defendants violated California state consumer protection statutes;

i. Whether Defendants were unjustly enriched by their conduct; and

j. Whether Plaintiff and Class Members are entitled to equitable relief, including injunctive relief.

94. A class action provides a fair and efficient method, if not the only method, for adjudicating this controversy. The substantive claims of the representative Plaintiff and the Class are nearly identical and will require evidentiary proof of the same kind and application of the same law. There is no plain, speedy, or adequate remedy other than by maintenance of this class action.

95. A class action is superior to other available methods for the fair and efficient adjudication of this controversy because Class Members number in the millions and individual joinder is impracticable. The expense and burden of individual litigation would make it impracticable or impossible for proposed Class Members to prosecute their claims individually. In contrast, a trial of Plaintiff and the Class Members' claims would be manageable as the common claims would require common proof. Unless the Class is certified, Defendants will remain free to continue to engage in the wrongful conduct alleged herein without consequence.

96. The persons in the Nationwide Class are in excess of 100,000 clients and are so numerous that the joinder of all such persons individually in this case is impracticable, and the disposition of their claims in this case and as part of a single class action lawsuit, rather than hundreds or thousands of individual lawsuits, will benefit the parties and greatly reduce the aggregate judicial resources that would be spent if this matter were handled as hundreds or thousands of separate lawsuits.

97. The persons in the California Subclass are believed to be in in excess of 12,374 clients, and are so numerous that the joinder of all such persons individually in

this case is impracticable, and the disposition of their claims in this case and as part of a single class action lawsuit, rather than hundreds or thousands of individual lawsuits, will benefit the parties and greatly reduce the aggregate judicial resources that would be spent if this matter were handled as hundreds or thousands of separate lawsuits.

98. Plaintiff knows of no difficulty that will be encountered in the management of this litigation, which would preclude its maintenance of a class action.

FIRST CAUSE OF ACTION

Violation of the Insurance Information and Privacy Protection Act, Ins. Code, § 791.01, *et seq.*

(On Behalf of Plaintiff and the Nationwide Class and the Nationwide Subclasses, or, alternatively, California Plaintiff and the California Subclass, against the California Defendants)

99. Plaintiff re-alleges and incorporates the paragraphs above as if fully set forth herein.

100. Plaintiff brings this claim on behalf of herself and the Nationwide Class and the Nationwide Subclasses, or, alternatively, herself and the California Subclass.

101. Defendants are subject to the requirements and mandates of the Insurance Information and Privacy Protection Act, Ins. Code, § 791.01, *et seq*.

102. Defendants are insurance institutions, agents or insurance-support organizations which collect, receive or maintain information in connection with insurance transactions which pertains to natural persons who are residents of this state, and/or engage in insurance transactions with applicants, individuals or policyholders who are residents of California in the course of providing life insurance, disability insurance and other related insurance products. Ins. Code, § 791.01

103. Defendants were obligated to provide notice of information practices to Plaintiff and Class Members in connection with insurance transactions. Defendants fulfilled this obligation by providing written notice at three key points: (1) upon delivering the insurance policy or certificate, as personal information had been

collected; (2) before or on the date of policy renewal or renewal confirmation; and (3) upon receiving requests for policy reinstatement or changes to insurance benefits. The notice detailed Defendants' retention and disclosure practices regarding Plaintiff's and Class Members' PII/PHI, whether personal information might be collected from third parties, the types of information collected, the methods and sources used, and the circumstances under which personal information could be disclosed without authorization. It also described the rights established under the Insurance Code, §§ 791.08 and 791.09, the process for exercising those rights, and the retention and disclosure practices of insurance-support organizations. Additionally, Defendants were required to disclose its **policies and practices with respect to protecting the confidentiality and security of nonpublic personal information**, including a general description as to who is authorized to have access to the information. Ins. Code, § 791.045(a)(1)-(2) citing Cal. Code Regs., tit. 10, § 2689.7.

104. Defendants violated IIPPA by unlawfully disclosing Plaintiff's and Class Members' personal and privileged information, including PI/PHI, to cyber criminals because of a data breach. This disclosure, caused by Defendants' wantonly, willfully and recklessly inadequate data security measures, occurred without Plaintiffs' and Class Members' written authorization, as required under the Insurance Code, §791.13(a) of the IIPPA. Defendants failed to ensure the confidentiality and integrity of sensitive information collected during insurance transactions, contravening the IIPPA's strict prohibitions against unauthorized disclosures absent a valid exception. By failing to implement reasonable safeguards to prevent unauthorized access, Defendants enabled cybercriminals to obtain Plaintiffs' and Class Members' PII and PHI, violating their statutory obligations under the IIPPA.

105. Defendants consciously disregarded the rights of Plaintiff and Class Members amounting to malice and/or willful intent, Civil Code § 3294, because Defendants' inadequate data security measures were brought to Defendants' attention before the Data Breach and Defendant, knowing that it possessed the PII/PHI of

Plaintiff and Class Members and their rights regarding the privacy and confidentiality of their PII/PHI intentionally ignored the warnings for profit motive reasons.

106. Motivated by pecuniary self-interests, Defendants intentionally failed to monitor its data systems continuously and run security audits, Defendants failed to implement multi-factor authentication for the employee and agent user accounts involved in the breach, allowing unauthorized access to PII/PHI and demonstrating a failure to adopt reasonable security measures. Defendants improperly granted excessive privileges to standard employee accounts, which allowed bad actors with access to use standard employee accounts to compromise other accounts within the system, supercharging their reach and the system's vulnerability. Further, Defendants designed their network in a manner that allowed compromised accounts to move laterally across the environment, permitting unauthorized access through PowerShell commands. Additionally, Defendants established a two-way trust relationship between their respective Active Directory domains, which facilitated the unauthorized sharing of Private Information across domains and further compromised system integrity. These failures were compounded by weak password practices, lack of employee training, unpatched vulnerabilities, poor access controls, inadequate data encryption, neglect of system updates, susceptibility to social engineering attacks and phishing scams, insider threats, and insufficient monitoring. Thus, Defendants consciously disregarded the rights of Plaintiff and Class Members.

107. Due to engaging in such conduct, Defendants have violated the Insurance Information and Privacy Protection Act, Ins. Code, § 791.01, *et seq*.

108. As a direct and proximate result of Defendants' above-described violations, Plaintiff and Class Members have suffered (and will continue to suffer) (a) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; (b) actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; (c) loss of the confidentiality of the stolen confidential data; (d) the illegal sale of the compromised data on the dark

web; (e) lost work time; and (f) loss of the benefit of the bargain, measured by the difference between the value of the services Plaintiff and Class Members paid for—services with adequate cybersecurity—and the actual value of the services provided, which lacked adequate security measures and practices; (g) other economic and non-economic harm.

109. Additionally, Plaintiff and Class Members seek and award for the cost of the action and reasonable attorneys' fees to the prevailing party pursuant to Insurance Code, § 791.20.

SECOND CAUSE OF ACTION

Unfair Competition Law, California Business and Professional Code Section 17200, *et seq*.

(On Behalf of Plaintiff and the Nationwide Class and the Nationwide Subclasses, or, alternatively, California Plaintiff and the California Subclass)

110. Plaintiff re-alleges and incorporates the paragraphs above as if fully set forth herein.

111. Plaintiff brings this claim on behalf of herself and the Nationwide Class and the Nationwide Subclasses, or, alternatively, the California Plaintiff and the California Subclass against only the California Defendants and the Arizona Plaintiff and the Arizona Subclass against the Arizona Defendants, Heritage, and Regal.

112. The California Unfair Competition Law, Cal. Bus. & Prof. Code §17200, *et seq*. ("UCL"), prohibits any "unlawful," "fraudulent," or "unfair" business act or practice and any false or misleading advertising, as defined by the UCL and relevant case law.

113. By reason of Defendants' above-described wrongful actions, inactions, and omissions, the resulting Data Breach, and the unauthorized disclosure of Plaintiff's and Class Members' PII/PHI, Defendants engaged in unlawful, unfair, and fraudulent practices within the meaning of the UCL.

114. Defendants' business practices, as alleged herein, were unfair because they

offend established public policy and are immoral, unethical, oppressive, unscrupulous and substantially injurious to consumers, in that the private and confidential PII/PHI of consumers has been compromised for all to see, use, or otherwise exploit.

115. Defendants' above-described wrongful actions, inaction, and omissions, the resulting Data Breach, and the unauthorized release and disclosure of Plaintiff's and Class Members' PII/PHI also constitute "unfair" business acts and practices within the meaning of Business & Professions Code sections 17200 *et seq.*, in that Defendants' conduct was substantially injurious to Plaintiff and Class Members, offensive to public policy, immoral, unethical, oppressive and unscrupulous, and the gravity of Defendants' conduct outweighs any alleged benefits attributable to such conduct.

116. Defendants engaged in unlawful acts and practices with respect to the services by establishing the sub-standard security practices and procedures described herein; by soliciting and collecting Plaintiff's and Class Members' PII/PHI with knowledge that the information would not be adequately protected; by violating the California Insurance Information and Privacy Protection Act, California Insurance Code, §§ 791–791.27; by violating the other statutes described herein, including California Consumer Privacy Act, California Civil Code § 1798.150, *et seq*., common law claims for negligence, breach of contract, breach of implied contract, breach of the implied covenant of good-faith and fair dealing, and invasion of privacy; and by storing Plaintiff's and Class Members' PII/PHI in an unsecure electronic environment in violation of IIPPA, which requires Defendants to take reasonable methods of safeguarding the PII/PHI of Plaintiff and the Class Members.

117. Defendants' practices were also unlawful and in violation of Civil Code sections 1798, *et seq*. and Defendants' own privacy policy because Defendants failed to take reasonable measures to protect Plaintiff's and Class Members' PII/PHI and failed to take remedial measures such as notifying its users when it first discovered that their PII/PHI may have been compromised.

118. In addition, Defendants engaged in unlawful acts and practices by failing

to disclose the Data Breach in a timely and accurate manner.

119. Defendants' business practices, as alleged herein, were fraudulent because they were likely to deceive consumers into believing that the PII/PHI they provided to Defendants would remain private and secure when, in fact, it was not private and secure.

120. Plaintiff and Class Members suffered (and continue to suffer) injury in fact and lost money or property as a direct and proximate result of Defendants' above-described wrongful actions, inactions, and omissions including, *inter alia*, the unauthorized release and disclosure of their PII/PHI.

121. But for Defendants' misrepresentations and omissions, Plaintiff and Class Members would not have provided their PII/PHI to Defendants or would have insisted that their PII/PHI be more securely protected.

122. As a direct and proximate result of Defendants' above-described wrongful actions, inactions, and omissions, the resulting Data Breach, and the unauthorized release and disclosure of Plaintiff and California Subclass members' PII/PHI, they have been injured by, *inter alia*: (1) the loss of the opportunity to control how their PII/PHI is used; (2) the diminution in the value and/or use of their PII/PHI entrusted to Defendants; (3) the compromise, publication, and/or theft of their PII/PHI; and (4) costs associated with monitoring their PII/PHI, amongst other things.

123. Plaintiff takes upon herself enforcement of the laws violated by Defendants in connection with the reckless and negligent disclosure of their PII/PHI. There is a financial burden incurred in pursuing this action, and it would be against the interests of justice to penalize Plaintiff by forcing them to pay attorneys' fees and costs from the recovery in this action. Therefore, an award of attorneys' fees and costs is appropriate under California Code of Civil Procedure § 1021.5.

THIRD CAUSE OF ACTION

California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.150, *et seq.*

(On Behalf of Plaintiff and the California Subclass Against the California Defendants)

124. Plaintiff re-alleges and incorporates the paragraphs above as if fully set forth herein.

125. The California Plaintiff brings this claim on behalf of herself and the California Subclass only.

126. Cal. Civ. Code § 1798.150(a) of the California Consumer Privacy Act ("CCPA") provides that "[a]ny consumer whose nonencrypted and nonredacted personal information, as defined in subparagraph (A) of paragraph (1) of subdivision (d) of Section 1798.81.5 . . . is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action" for statutory damages, actual damages, injunctive relief, declaratory relief and any other relief the court deems proper.

127. Defendants have long been aware of Plaintiff's allegations, claims, and demands, including through Plaintiff Price's correspondence, which provided notice in compliance with the CCPA in December 20, 2024. Further, Defendants are the parties with the most knowledge of the underlying facts giving rise to Plaintiff's allegations, so that any pre-suit notice would not put Defendants in a better position to evaluate those claims.

128. Plaintiff and California Subclass members are "consumers" as defined by Cal. Civ. Code § 1798.140(g) because they are natural persons who reside in California.

129. Defendants are "business[es]" as defined by Cal. Civ. Code § 1798.140(c) because Defendants are corporations organized for the profit or financial benefit of their shareholders or owners and have gross annual revenues in excess of twenty-five million dollars.

130. Plaintiff and California Subclass members provided Defendants with their nonencrypted and nonredacted personal information as defined in § 1798.81.5 in the form of their PII/PHI. This PII/PHI included each of their names, social security

number, address, date of birth, sensitive medical data, and phone number. These allegations cover all information

131. Defendants failed to take sufficient and reasonable measures to safeguard their data security systems and protect Plaintiff's and California Subclass members' highly sensitive personal information and medical data from unauthorized access. Defendants' failure to maintain adequate data protections subjected Plaintiff's and the California Subclass members' nonencrypted and nonredacted sensitive personal information to exfiltration and disclosure by malevolent actors.

132. The unauthorized access, exfiltration, theft, and disclosure of Plaintiff and the California Subclass members' PII/PHI was a result of Defendants' violation of its duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information.

133. Under Defendants' duty to protect customers' PII/PHI, it was required to implement reasonable security measures to prevent and deter hacks from accessing the PII/PHI of its customers. That these vulnerabilities existed and enabled unauthorized third parties to access and harvest customers' PII/PHI evidence that Defendants have breached that duty.

134. Plaintiff and California Subclass members have suffered actual injury and are entitled to damages in an amount to be proven at trial but in excess of the minimum jurisdictional requirement of this Court.

135. Defendants' violations of Cal. Civ. Code § 1798.150(a) are a direct and proximate result of the Data Breach.

136. Plaintiff and California Subclass members seek all monetary and non-monetary relief allowed by law, including actual or nominal damages; statutory damages pursuant to Cal. Civ. Code § 1798.150(a)(1)(A) in an amount not less than one hundred dollars ($100) and not greater than seven hundred and fifty ($750) per consumer per incident or actual damages, whichever is greater; declaratory and injunctive relief, including an injunction barring Defendants from disclosing their

PHI/PII without their consent; reasonable attorneys' fees and costs; and any other relief that is just and proper.

FOURTH CAUSE OF ACTION

Negligence

(On Behalf of Plaintiff and the Nationwide Class and the Nationwide Subclasses, or, alternatively, the California Plaintiff and the California)

137. Plaintiff re-alleges and incorporates the paragraphs above as if fully set forth herein.

138. Plaintiff brings this claim on behalf of herself and the Nationwide Class and the Nationwide Subclasses, or, alternatively, the California Plaintiff and the California Subclass and the Arizona Plaintiff and the Arizona Subclass.

139. Plaintiff and Class Members were required to provide Defendants with their PII/PHI to receive services. Defendants collected and stored this information, including their names and one or more of the following: address, insurance information, date of birth, and clinical information, such as diagnosis, procedure, and/or prescription information.

140. Defendants had a duty to Plaintiff and Class Members to safeguard and protect their PII/PHI.

141. Defendants assumed a duty of care to use reasonable means to secure and safeguard this PII/PHI, to prevent its disclosure, to guard it from theft, and to detect any attempted or actual breach of its systems.

142. Defendants had full knowledge about the sensitivity of Plaintiff and Class Members' PII/PHI, as well as the type of harm that would occur if such PII/PHI were wrongfully disclosed.

143. Defendants had a duty to exercise reasonable care in safeguarding, securing and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining and testing its security protocols to ensure that PII/PHI

in its possession was adequately secured and protected and that employees tasked with maintaining such information were adequately training on relevant cybersecurity measures.

144. Plaintiff and Class Members were the foreseeable and probable victims of any inadequate security practices and procedures. Defendants knew of or should have known of the inherent risks in collecting and storing the PII/PHI of Plaintiff and Class Members, the critical importance of providing adequate security of that PII/PHI, the current cyber scams being perpetrated, and that they had inadequate employee training and education and IT security protocols in place to secure the PII/PHI of Plaintiff and Class Members.

145. Defendants' own conduct created a foreseeable risk of harm to Plaintiff and Class Members. Defendants' misconduct included, but was not limited to, their failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendants' misconduct also included their decision not to comply with HIPAA and industry standards for the safekeeping and encrypted authorized disclosure of the PII/PHI of Plaintiff and Class Members.

146. Plaintiff and Class Members had no ability to protect their PII/PHI that was in Defendants' possession.

147. Defendants were able to protect against the harm suffered by Plaintiff and Class Members because of the Data Breach.

148. Defendants had a duty to put proper procedures in place to prevent the unauthorized dissemination of Plaintiff's and Class Members' PII/PHI.

149. Defendants have admitted that Plaintiff's and Class Members' PII/PHI was wrongfully disclosed to unauthorized third persons because of the Data Breach.

150. Defendants breached their duty of care by failing to secure and safeguard the PII/PHI of Plaintiff and Class Members. Defendants negligently stored and/or maintained their data security systems and made that information available to unauthorized parties accessible through the Internet.

151. Further, Defendants by and through their above negligent actions and/or inactions, breached their duties to Plaintiff and Class Members by failing to design, adopt, implement, control, manage, monitor and audit its processes, controls, policies, procedures and protocols for complying with the applicable laws and safeguarding and protecting Plaintiff's and Class Members' PII/PHI within their possession, custody and control.

152. Plaintiff and the other Class Members have suffered harm because of Defendants' negligence. These victims' loss of control over the compromised PII/PHI subjects each of them to a greatly enhanced risk of identity theft, fraud, and myriad other types of fraud and theft stemming from either use of the compromised information, or access to their user accounts.

153. It was reasonably foreseeable – in that Defendants knew or should have known – that their failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class Members' PII/PHI would result in its release and disclosure to unauthorized third parties who, in turn wrongfully used such PII/PHI, or disseminated it to other fraudsters for their wrongful use and for no lawful purpose.

154. But for Defendants' negligent and wrongful breach of their responsibilities and duties owed to Plaintiff and Class Members, these clients' PII/PHI would not have been compromised.

155. As a direct and proximate result of Defendants' above-described wrongful actions, inactions, and omissions, the resulting Data Breach, and the unauthorized release and disclosure of Plaintiff's and Class Members' PII/PHI, they have incurred (and will continue to incur) actual injury and harm for which they are entitled to compensation. Defendants' wrongful actions, inactions, and omissions constituted (and continue to constitute) common law negligence/negligent misrepresentation.

156. Violations of statutes which establish a duty to take precautions to protect a particular class of persons from a particular injury or type of injury may constitute negligence *per se*.

157. Defendants' violation of IIPPA may constitute negligence *per se*.

158. The Insurance Information and Privacy Protection Act (IIPPA) prohibits insurance companies, agents, and support organizations from disclosing personal information collected during an insurance transaction without the individual's consent. This means personal details cannot be shared with third parties unless specific conditions are met, such as legitimate business purposes or written authorization. IIPPA restricts unauthorized sharing of personal information related to insurance applications and claims, including prohibiting unrestricted disclosure without a valid reason and consent, barring the use of personal information for marketing purposes without explicit agreement, and restricting the disclosure of information beyond what is necessary for processing insurance applications or claims. Defendants' failure to comply with IIPPA is negligence *per se.*

159. Plaintiff and Class Members are within the class of persons that IIPPA privacy laws were intended to protect.

160. The harm Plaintiff and Class Members suffered because of the Data Breach is the type of harm the IIPPA was intended to guard against.

161. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Ambry, of failing to use reasonable measures to protect PII/PHI. The FTC publications and orders described above also form part of the basis of Defendants' duty in this regard. This informs the standard of care that Defendants must exercise in safeguarding PII/PHI.

162. Defendants violated Section 5 of the FTC Act by failing to use reasonable measures to protect Plaintiff's and Class Members' PII/PHI and not complying with applicable industry standards, as described in detail herein. Defendants' conduct was particularly unreasonable given the nature and amount of PII/PHI they obtained and stored, and the foreseeable consequences of a data breach including, specifically, the damages that would result to Plaintiff and Class Members.

163. HIPAA privacy laws were enacted with the objective of protecting the confidentiality of patients' healthcare information and set forth the conditions under which such information can be used, and to whom it can be disclosed. HIPAA privacy laws not only apply to healthcare providers and the organizations they work for, but to any entity that may have access to healthcare information about a patient that—if it were to fall into the wrong hands—could present a risk of harm to the patient's finances or reputation. This informs the standard of care that Defendants must exercise in safeguarding PII/PHI.

164. Additionally, as a direct and proximate result of Defendants' negligence *per se*, Plaintiff and Class Members have suffered and will suffer the continued risks of exposure of their PII/PHI, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII/PHI in its continued possession.

165. As a direct and proximate result of Defendants' above-described violations, Plaintiff and Class Members have suffered (and will continue to suffer) (a) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; (b) actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; (c) loss of the confidentiality of the stolen confidential data; (d) the illegal sale of the compromised data on the dark web; (e) lost work time; and (f) loss of the benefit of the bargain, measured by the difference between the value of the services Plaintiff and Class Members paid for—services with adequate cybersecurity—and the actual value of the services provided, which lacked adequate security measures and practices; (g) other economic and non-economic harm; anxiety, emotional distress, loss of privacy, and other non-economic losses, and are entitled to damages for their non-economic damages in an amount to be proven at trial.

//

//

FIFTH CAUSE OF ACTION

Breach of Contract

(On Behalf of Plaintiff and the Nationwide Class and the Nationwide Subclasses, or, alternatively, the California Plaintiff and the California Subclass)

166. Plaintiff re-alleges and incorporates the paragraphs above as if fully set forth herein.

167. Plaintiff brings this claim on behalf of herself and the Nationwide Class and the Nationwide Subclasses, or, alternatively, herself and the California Subclass.

168. Plaintiff and Class Members entered a contract with Defendants for the provision of medical and/or other services.

169. The terms of Defendants' privacy policy and other documents identified above are components of the contract.

170. Plaintiff and Class Members performed substantially all that was required of them under their contract with Defendants, or they were excused from doing so.

171. Defendants failed to perform their obligations under the contract, including by failing to provide adequate privacy, security, and confidentiality safeguards for Plaintiff and Class member's information and documents.

172. As a direct and proximate result of Defendants' breach of contract, Plaintiff and Class Members did not receive the full benefit of the bargain and, instead, received medical and/or other services that were less valuable than described in their contracts. Plaintiff and Class Members, therefore, were damaged in an amount at least equal to the difference in value between that which was promised and Defendants' deficient performance.

173. Also, because of Defendants' breach of contract, Plaintiff and Class Members have suffered actual damages resulting from the exposure of their personal information, and they remain at imminent risk of suffering additional damages in the future.

174. Accordingly, Plaintiff and Class Members have been injured by

Defendants' breach of contract and are entitled to damages and /or restitution in an amount to be proven at trial.

SIXTH CAUSE OF ACTION

Breach of Implied Contract

(On Behalf of Plaintiff and the Nationwide Class and the Nationwide Subclasses, or, alternatively, the California Plaintiff and the California Subclass)

175. Plaintiff re-alleges and incorporates the paragraphs above as if fully set forth herein.

176. Plaintiff brings this claim on behalf of herself and the Nationwide Class and the Nationwide Subclasses, or, alternatively, herself and the California Subclass.

177. Through their course of conduct, Defendants, Plaintiffs, and Class Members entered implied contracts for Defendants to implement data security adequate to safeguard and protect the privacy of Plaintiff's and Class Members' PHI/PII.

178. As part of this contract, Defendants required Plaintiff and Class Members to provide and entrust to Defendant, *inter alia*, names, Social Security numbers, dates of birth, address, diagnosis and treatment information, laboratory test results, prescription data, radiology reports, health plan member numbers, phone numbers.

179. Defendants solicited and invited Plaintiff and Class Members to provide their PHI/PII as part of Defendants' regular business practices. Plaintiff and Class Members accepted Defendants' offers and provided their PHI/PII thereto.

180. As a condition of being clients thereof, Plaintiff and Class Members provided and entrusted their PHI/PII to Defendants. In so doing, Plaintiff and Class Members entered implied contracts with Defendants by which Defendants agreed to safeguard and protect such non-public information, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and Class Members if their data had been breached and compromised or stolen.

181. A meeting of the minds occurred when Plaintiff and Class Members agreed to, and did, provide their PHI/PII to Defendants, in exchange for, amongst other things,

the protection of their PHI/PII.

182. Plaintiff and Class Members fully performed their obligations under the implied contracts with Defendants.

183. Defendants breached the implied contracts they made with Plaintiff and Class Members by failing to safeguard and protect their PHI/PII and by failing to provide timely and accurate notice to them that their PHI/PII was compromised because of the Data Breach.

184. As a direct and proximate result of Defendants' above-described breach of implied contract, Plaintiff and Class Members have suffered (and will continue to suffer) (a) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; (b) actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; (c) loss of the confidentiality of the stolen confidential data; (d) the illegal sale of the compromised data on the dark web; (e) lost work time; and (f) other economic and non-economic harm.

SEVENTH CAUSE OF ACTION

Breach of the Implied Covenant of Good-Faith and Fair Dealing

(On Behalf of Plaintiff and the Nationwide Class and the Nationwide Subclasses, or, alternatively, the California Plaintiff and the California Subclass)

185. Plaintiff re-alleges and incorporates the paragraphs above as if fully set forth herein.

186. Plaintiff brings this claim on behalf of herself and the Nationwide Class and the Nationwide Subclasses, or, alternatively, herself and the California Subclass.

187. As described above, Plaintiff and Class Members entered valid, binding, and enforceable express or implied contracts with Defendants, and Defendants made promises and representations to Plaintiff and the Class that it would comply with HIPAA and other applicable laws and industry best practices.

188. These promises and representations became a part of the contract between

Plaintiff and Class Members.

189. While Defendants had discretion in the specifics of how it met the applicable laws and industry standards, this discretion was governed by an implied covenant of good faith and fair dealing

190. The contracts under which Plaintiff and Class Members were intended beneficiaries were subject to implied covenants of good faith and fair dealing requiring all parties to act in good faith and with reasonable efforts to perform their contractual obligations (both explicit and fairly implied) and not to impair the rights of the other parties to receive the rights, benefits, and reasonable expectations under those contracts. These implied covenants required Defendants to act fairly and in good faith in carrying out their contractual obligations to take reasonable measures to protect Plaintiff's PII/PHI from unauthorized disclosure and to comply with state laws and regulations.

191. Defendants breached this implied covenant when it engaged in acts and/or omissions that are declared unfair trade practices by the FTC and state statutes and regulations, and unlawful practices by IIPPA and CCPA.

192. Plaintiff and Class Members did all or substantially all the significant things that the contract required them to do.

193. Likewise, all conditions required for Defendants' performance were met.

194. Defendant's acts and omissions unfairly interfered with Class Members' rights to receive the full benefit of their contracts.

195. A "special relationship" existed between Defendants and the Plaintiff and Class Members. Defendants entered a "special relationship" with Plaintiff and Class Members who sought medical services or treatment at Regal's affiliated facilities and, in doing so, entrusted Defendants, pursuant to their requirements and the privacy policy and related documents, with their PII/PHI.

196. Despite this special relationship with Plaintiff and Class Members, Defendants did not act in good faith and with fair dealing to protect Plaintiff's and Class Members' PII/PHI.

197. Plaintiff and Class Members performed all conditions, covenants, obligations, and promises owed to Defendants.

198. Defendants' failure to act in good faith in complying with the contracts denied Plaintiff and Class Members the full benefit of their bargain. This failure resulted in Plaintiff and Class Members receiving services that were less valuable than what they paid for and less valuable than their reasonable expectations.

199. Class Members have been harmed by Defendants' breach of this implied covenant in the many ways described above, including overpayment for products and services, actual identity theft and/or imminent risk of devastating identity theft that exists now that cyber criminals have their Personal and Medical Information, and the attendant long-term expense of attempting to mitigate and insure against these risks.

200. Accordingly, Plaintiff and Class Members have been injured because of Defendants' breach of the covenant of good faith and fair dealing and are, thus, entitled to damages and/or restitution in an amount to be proven at trial.

EIGHTH CAUSE OF ACTION

Invasion of Privacy

(On Behalf of Plaintiff and the Nationwide Class and the Nationwide Subclasses, or, alternatively, the California Plaintiff and the California Subclass)

201. Plaintiff re-alleges and incorporates the paragraphs above as if fully set forth herein.

202. Plaintiff brings this claim on behalf of herself and the Nationwide Class and the Nationwide Subclasses, or, alternatively, herself and the California Subclass.

203. Plaintiff and Class Members have a legally protected privacy interest in their PII/PHI that Defendants required them to provide and allow them to store.

204. California established the right to privacy in Article 1, Section 1 of the California Constitution.

205. The State of California recognizes the tort of Intrusion into Private Affairs, and adopts the formulation of that tort found in the Restatement (Second) of Torts which

states:

> One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person. Restatement (Second) of Torts § 652B (1977)

206. Plaintiff and Class Members reasonably expected that their PII/PHI would be protected and secured from unauthorized parties, would not be disclosed to any unauthorized parties or disclosed for any improper purpose.

207. Defendants owed a duty to clients in their network, including Plaintiff and Class Members, to keep their PII/PHI confidential.

208. The unauthorized disclosure of PII/PHI, especially the type related to personal health information, is highly offensive to a reasonable person.

209. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiff and Class Members disclosed their PII/PHI to Defendants as part of their use of Defendants' services, but privately, with the intention that the PII/PHI would be kept confidential and protected from unauthorized disclosure. Plaintiff and Class Members were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

210. The Data Breach constitutes an intentional interference with Plaintiff's and Class Members' interest in solitude or seclusion, either as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

211. Defendants acted with a knowing state of mind when they permitted the Data Breach because they knew its information security practices were inadequate and would likely result in a data breach such as the one that harmed Plaintiff and Class Members.

212. Acting with knowledge, Defendants had notice and knew that their inadequate cybersecurity practices would cause injury to Plaintiff and Class Members.

213. Defendants unlawfully invaded the privacy rights of Plaintiff and Class

Members by (a) failing to adequately secure their PII/PHI from disclosure to unauthorized parties for improper purposes; (b) disclosing their PII/PHI to unauthorized parties in a manner that is highly offensive to a reasonable person; and (c) disclosing their PII/PHI to unauthorized parties without the informed and clear consent of Plaintiff and Class Members. This invasion into the privacy interest of Plaintiff and Class Members is serious and substantial.

214. In failing to adequately secure Plaintiff's and Class Members' PII/PHI, Defendants acted in reckless disregard of their privacy rights. Defendants knew or should have known that their substandard data security measures are highly offensive to a reasonable person in the same position as Plaintiff and Class Members.

215. Defendants violated Plaintiff's and Class Members' right to privacy under the common law as well as under state law, including the California Constitution, Article I, Section I. As a direct and proximate result of Defendants' unlawful invasions of privacy, Plaintiff's and Class Members' PII/PHI has been viewed or is at imminent risk of being viewed, and their reasonable expectations of privacy have been intruded upon and frustrated. Plaintiff and the proposed Class have suffered injury because of Defendants' unlawful invasions of privacy and are entitled to appropriate relief.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff and the Class(es) pray for judgment as follows:

1. For an Order certifying the proposed Class and any appropriate Subclasses, pursuant to Fed. R. Civ. P. 23(a), 23(b)(2), and 23(b)(3), requiring notice thereto to be paid by Defendants and appointing Plaintiff and their counsel to represent the Class(es);

2. For appropriate injunctive relief and/or declaratory relief, including, but not limited to, an order requiring Defendants to immediately secure and fully encrypt all confidential information, to store any computer passwords in a location separate from the computers, to cease negligently storing, handling, and securing their clients' confidential information, to notify clients whose medical information was wrongly disclosed in an expedient and timely manner and to provide identity theft monitoring

for an additional five years;

3. Adjudging and decreeing that Defendants have engaged in the conduct alleged herein;

4. For compensatory and general damages according to proof on certain causes of action;

5. For damages on certain causes of action, including violation of California Insurance Code, § 791.01, *et seq*; in an amount not less than one hundred dollars ($100) and not greater than seven hundred and fifty ($750) per consumer per incident or actual damages, whichever is greater pursuant to § 1798.150(a)(1)(A); and all other damages and statutory remedies available by statute or law;

6. For reimbursement, restitution and disgorgement on certain causes of action;

7. For both pre- and post-judgment interest at the maximum allowable rate on any amounts awarded;

8. For costs of the proceedings herein;

9. For reasonable attorneys' fees, as allowed by statute; and

10. For any and all such other and further relief that this Court may deem just and proper, including, but not limited to, punitive or exemplary damages.

Dated: December 20, 2024

Respectfully Submitted,

/s/ *Thiago M. Coelho*
Thiago M. Coelho
Shahin Rezvani
WILSHIRE LAW FIRM, PLC
Attorneys for Plaintiffs and the Putative Class

DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury of all issues in this action so triable of right.

Dated: December 20, 2024

Respectfully Submitted,

/s/ *Thiago M. Coelho*
Thiago M. Coelho
Shahin Rezvani
WILSHIRE LAW FIRM, PLC
Attorneys for Plaintiffs and the Putative Class